National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Arbor Networks
Peakflow X Version 3.1.4

Report Number: CCEVS-VR-05-0112
Dated: 2 November 2005

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Catalina Gomolka
Mitretek Systems
Falls Church, Virginia

Common Criteria Testing Laboratory
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, Maryland 21046

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of Arbor Peakflow X Version 3.1.4. The TOE, Arbor Networks Peakflow X version 3.1.4, is a network integrity system (NIS) consisting of collector and controller appliances. The collectors capture network traffic information in order to build and monitor network usage policies. The controller enables management of network usage policy definitions and provides access to the results of its monitoring of adherence by network entities to the defined policies. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by Science Applications International Corporation (SAIC) and was completed 2 November 2005. The information in this report is largely derived from an Evaluation Technical Report (ETR) written by SAIC and submitted to the Validator. The evaluation determined that the product conforms to the CC Version 2.1, Part 2 extended and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE, Peakflow X version 3.1.4, is intended for use in large enterprise networks. Peakflow X allows organizations to identify and address internal security issues. Peakflow X constructs a holistic view of the entire network by clustering hosts into groups based on their operational policy. Using this view, Peakflow X generates indications, warnings and alerts of anomalous behavior that may indicate the presence of zero-day threats, worms, misuse, or abuse.

Peakflow X first establishes an effective-use policy for the network, as it is defined by an audit of its ongoing traffic patterns. Peakflow X then constantly reconciles that policy against actual network use. As the system detects and reports anomalies, the administrator can decide whether to act on these detected anomalous uses of the network, or to adjust the policy, further refining the derived usage policy.

Peakflow X derives its initial policy by learning network behaviors. It accomplishes this by watching the flow of information on the attached network and recording a set of behaviors. Then, once the administrator initiates grouping, Peakflow X automatically groups hosts that have similar behaviors, thus defining the policy for expected network use. The administrator can also refine the group memberships to reflect additional subtleties of network behavior, and define additional flow rules. The policy can be expressed in either positive or negative terms so flow connections can be either explicitly permitted or denied.

Once grouping is complete and the administrator has determined that the learning phase has sufficiently captured the network traffic data, the administrator switches Peakflow X from learning to active mode.

At this point, Peakflow X starts observing actual network traffic and reporting any network use that represents policy violation. All flow information is stored in a traffic flow log, available for subsequent anomaly or traffic flow analysis. When Peakflow X detects a policy violation, it generates events that trigger interactive or synchronous policy refinements.

The administrator can then choose to:

- Accept the anomaly as an acceptable use, which updates the policy
- Explicitly forbid the behavior, which updates the policy
- Ignore the anomaly and defer modifying the policy.

When the administrator accepts or denies a flow rule, they either accept the specific host-host rule, or a more general host-group or group-group rule. The administrator can also refine policy by manually entering a flow rule that may actually correspond to a type of traffic the system has not yet seen.

Other important events, such as port scans or new hosts appearing on the network, also generate alerts, and the administrator can address these issues individually, or in batch mode.

The TOE provides the administrator with notification of potential violations of the specified network behavior policies. The TOE does not directly implement any traffic flow or access control policies on the backbone network that it monitors. It is the responsibility of the administrator to take appropriate action based upon the specific notification or alert that is received.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- the organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Evaluation Identifiers for Arbor Peakflow X Version 3.1.4	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Arbor Peakflow X Version 3.1.4
Protection Profile	N/A
Security Target	Arbor Peakflow X Security Target, Version 1.0, dated 8 July 2005 [9]
Evaluation Technical Report	Evaluation Technical Report (ETR) for Arbor Networks Peakflow X Version 3.1.4, (Version 1.1) dated 2 November 2005 [10]
Conformance Result	Part 2 extended and Part 3 conformant, and EAL2
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable International Interpretations effective on 24 March 2004
Version of CEM	CEM Version 1.0 [5], [6], and all applicable International Interpretations effective on 24 March 2004.
Sponsor	Arbor Networks, Inc 430 Bedford Street, Suite 160 Lexington, MA 02420
Developer	Arbor Networks, Inc 430 Bedford Street, Suite 160 Lexington, MA 02420
Evaluator(s)	**Science Applications International Corporation** Anthony J. Apted Terrie Diaz Craig Floyd Suzanne Hamilton
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers Catalina Gomolka

2.1 Applicable Interpretations

The CCTL Evaluation Team performed an analysis of those International Interpretations that were in place when the evaluation began on 24 March 2004 and determined that the following were applicable to this evaluation.

International Interpretations

RI#003 – Unique identification of configuration items in the configuration list (11 February 2002)

RI#038 – Use of “As a minimum” in C & P elements (31 October 2003)

RI#043 – Meaning of “clearly stated” in APE/ASE OBJ.1 (16 February 2001)

RI#051– Use of documentation without C & P elements (11 February 2002)

RI#084 – Aspects of objectives in TOE and environment (31 July 2001)

RI#085 – SOF Claims additional to the overall claim (11 February 2002)

RI#116 – Indistinguishable work units for ADO_DEL (31 July 2001)

.

3 Security Policy

The TOE implements several security policies to ensure its reliability as a network integrity tool. Those policies deal with restrictions on the persons that may administer the TOE, access to the information collected by the TOE, and the integrity of the information collected by the TOE. The TOE does not directly participate in the enforcement of any access control policies on the underlying network in which it is intended to operate. It provides information about network activity that can be used to more securely administer the backbone network. An overview of the security policies implemented by the TOE is provided in the following four subsections. A more detailed description of the policies is available in the ST [9]

3.1 Identification and Authentication

Both the Controller and Collector components require that administrators must be identified and authenticated before allowing them to perform any other functions. Peakflow X associates a “userid” and authentication data with each user.

3.2 Security Management

PeakflowX defines a single security management role of Administrator. The Administrator is able to manage the behavior of the network monitoring policy, by switching it between learning and monitoring modes, as well as manage user accounts to control access to the Peakflow X appliances. The Administrator is able to modify the rules that specify the network monitoring policy.

3.3 Protection of the TSF

Peakflow X protects from disclosure the traffic flow data transmitted by Collectors to the Controller. Data may be transmitted through a dedicated management network or over the monitored network, but in either case the communications between the Collectors and the Controller is protected by SSL. The TOE also detects modifications to traffic flow data transmitted by Collectors to the Controller and discards modified data. The TOE ensures that its security functions cannot be bypassed. All network traffic that is collected (either by a Collector or by the Controller in a Controller-only installation) is summarized as a traffic flow and used to build the network monitoring policy (in learning mode) or is compared against the network monitoring policy for anomalous behavior (in active mode). Peakflow X is implemented on dedicated network appliances and, as such, maintains a domain for its own execution. It protects itself against tampering by presenting limited, well-defined and -controlled external interfaces.

3.4 Network Integrity System

Peakflow X monitors network traffic and distills captured network information (either raw packets or NetFlow data) into traffic flow data. Peakflow X uses this traffic flow data to build a policy of allowed network flows and then monitors network traffic against this policy. Peakflow X generates alerts if it identifies: a traffic flow that is inconsistent with the network monitoring policy; a traffic flow involving a previously unknown host; a traffic flow indicating an unauthorized scan; a traffic flow indicating an unusual increase in traffic volumes.

Peakflow X operates using a high-level representation of observed traffic. It records individual connections on the attached network (flows), and groups of related connections (sessions). Peakflow X identifies individual flows using flow rules that capture the significant aspects of the connection. Flow rules can include network host IP addresses, network service ports (for protocols such as UDP or TCP, or ICMP) types and codes. Flow rules identify both ongoing and historical traffic and they can be used to describe the network policy – which operations are permitted and which operations are denied within the network. In the case of ongoing and historical traffic, flow rules are augmented with usage statistics, including total numbers of bytes flowing in and out of a connection.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The evaluation made a set of assumptions concerning the product usage that characterize the physical protection of the system as well as the training and behavior of system administrators and users. The evaluation depended upon the following objectives being met for the environment in which the TOE is used:

The TOE appliances must be installed and configured in their target networks so that all applicable network traffic will be directed to the appliances.

The TOE appliances must be installed, configured, and managed by suitable administrator personnel in accordance with the applicable guidance documentation.

The TOE appliances and their connections must be protected from unauthorized physical access and potential tampering.

4.2 Clarification of Scope

The TOE provides the administrator with notification of potential violations of the specified network behavior policies. The TOE does not directly implement any traffic flow or access control policies on the backbone network that it monitors. It is the responsibility of the administrator to take appropriate action based upon the specific notification or alert that is received.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE consists of a Controller appliance and zero or more Collector appliances. The role of the Collector is to collect all network traffic, either as raw network packets (via a SPAN - Switched Port Analyzer - port) or as NetFlow[1] information. The Collector summarizes network traffic into flow information, which is then passed to the Controller.

The Controller receives the summarized flow information from one or more Collectors (or generates this information itself in an installation without any Collectors). While in learning mode, the Controller uses the flow information to build up its view of the network and its behavior. When in active mode, it compares flow information against its model of the network and generates alerts if it detects anomalous behavior. All flow information is stored in a traffic flow log, available for subsequent anomaly or traffic flow analysis.

Both the Collector and Controller appliances are based on Intel commodity servers and utilize the Arbor Networks Operating System (ArbOS), which is based on OpenBSD.

Both of the appliances provide external network interfaces. One network interface is used to collect network traffic flow information via a SPAN port or Netflow from an existing network device such as a router. The second network interface is used for administration and to isolate administration traffic from the network that is being monitored. Either network interface can be configured to carry network traffic flow information between Collector and Controller appliances, but that communication is protected using SSL regardless.

6 Delivery and Documentation

The TOE is purchased as Controller appliance and zero or more Collector appliances. The Controller appliance and Collector appliances may be separately acquired. The part numbers for the appliances are:

PeakflowX Controller	PKF-X-CN
PeakflowX Collector	PKF-X-CL

To obtain the evaluated version of the TOE, the purchaser must specify that they want Version 3.1.4.

[1] Cisco IOS® NetFlow technology is an integral part of Cisco IOS Software that collects and measures data as it enters specific routers or switch interfaces.

Prior to delivery to the customer there is some customer specific information that must be programmed into the appliances by the developer. Hence, some aspects of the eventual deployment must be known at the time the products are acquired. The customer must provide the following information on a Pre-Build Questionnaire for developer programming into the appliances

> Certificate Identifiers, if certificates are to be used for correspondence between the Controller and the Collectors
>
> Hostname for the platform
>
> Platform type
>
> Initial Password
>
> IP address and mask for each interface
>
> Default route
>
> List of network prefixes allowed access by protocol (https, ping, BGP, Telnet, SSH)
>
> NTP server address
>
> Time Zone
>
> Additional information regarding power type and associated connectors.

There is one hardcopy document that is also delivered as part of the TOE. This document, The *Peakflow X Installation and User Guide version 3.1.4 (PX-UG-314)* is the only documentation needed to setup and administer the delivered TOE.

7 IT Product Testing

7.1 Developer Testing

Arbor Networks developed a suite of tests specifically for this evaluation. The developer already maintained a suite of tests for confirming that the Peakflow X product met its functional requirements. However, some of the developer's tests were designed to be carried out on live customer networks that included heavy network traffic. Some of that testing did not lend itself well to the types of records and repeatability that was needed for the CC evaluation because the capturing and replaying of all of the network traffic for some of the vendors original tests was not conveniently achievable in the CCTL test environment. After an evaluation team analysis of the existing testing, the developer generated additional data to ensure that all of the security functions could be tested in a manner that could be analyzed and repeated by the evaluation team.

Arbor Networks provided test documentation that described how each of the TOE security functions is tested including a test plan, test procedures, expected results and the actual results of applying the tests. The test configuration that is used by Arbor

Networks for those tests that are used to meet Common Criteria requirements is similar to the one described in the following section for the testing that was performed by the evaluation team.

The evaluators were provided with the complete set of test documentation. The evaluators checked that each of the test cases supported the security functions to which it was mapped and that the expected test results matched the actual test results. The Evaluators determined that the "Pass" meant that the expected results where achieved and the TOE behaved as expected.

7.2 Evaluator Testing

CCTL evaluation team testing was conducted at the CCTL facility in Columbia, MD in a couple of sessions. Initial testing took place in November 2004. The initial testing identified previously mentioned problems with the process of replaying of captured network traffic. Further testing was performed in December of 2004 after the vendor had developed alternate test data that permitted the evaluators to repeat vendor tests and compare expected results against the actual results of the tests. Additional supplemental testing was performed in October 2005 to further exercise the collection interfaces on the Controller appliance.

During testing the evaluators performed the following actions:

1. Execution of most of the developer's functional tests
2. Independent Testing
3. Vulnerability Testing (AVA_VLA.1)

Evaluator testing was observed by the validation team and there were no vendor representatives present during evaluation team testing.

The test configuration is illustrated in **Figure 1: Evaluation Test Configuration** on page 12.The primary test configuration used by the evaluation team had one controller and one collector. The TOE was also tested in a configuration without a separate collector appliance. In the latter configuration, the Controller was configured to function as a collector as well as a controller. Microsoft Window XP based computers were connected to the controller and the collector through serial ports for the purpose of administering those appliances. Those computers were also directly connected to the local network to perform network based operations. The Linux host was used to replay traffic and the HP host was used to run a vulnerability scanning tool. The following software was used in the test configuration:

- tcpdump for packet collection; trafgen for traffic generation; tcpreplay for packet replay; ssh client (on Linux laptop packet replay machine)
- Internet Explorer; telnet client; Microsoft Hyper Terminal 5.1 (on XP desktop and XP laptop)
- DNS server; SMTP server (on Compaq)
- Nessus open source vulnerability scanner (on HP laptop).

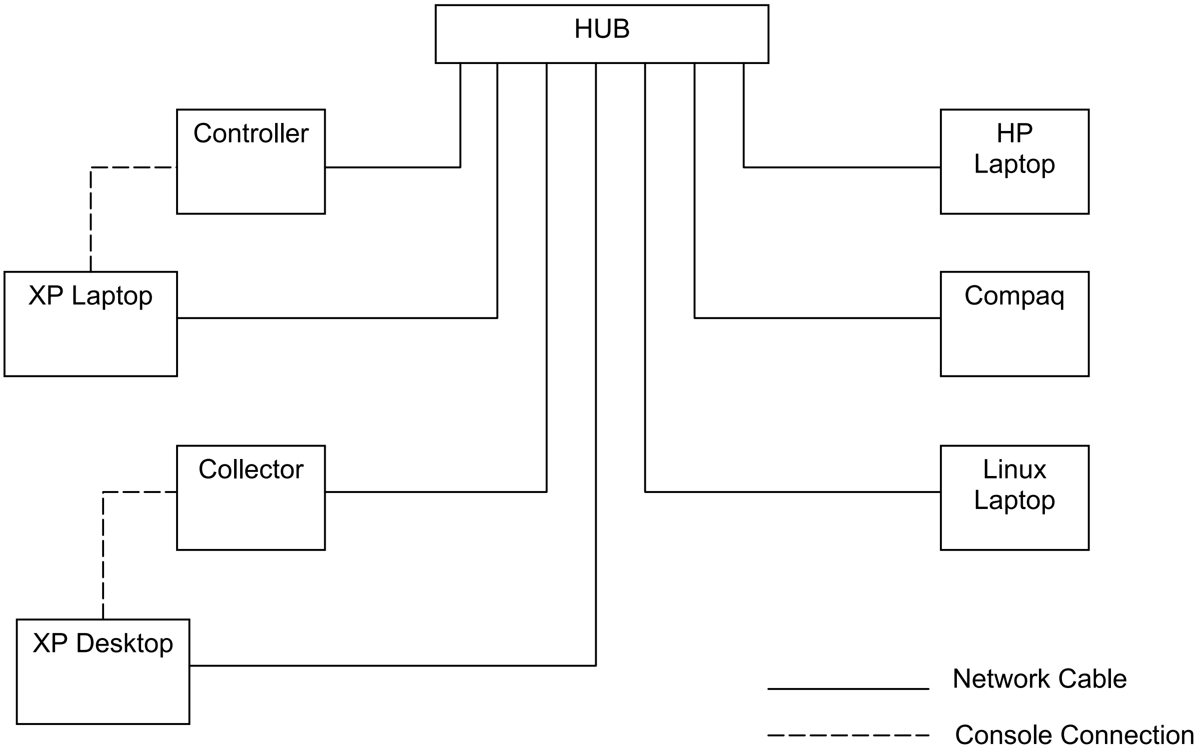

Figure 1: Evaluation Test Configuration

The evaluation team independently executed all of vendor test procedures other than two tests (for Syslog and SNMP alerts) that could not be performed in the test configuration, and a test that was deemed to be redundant with the other tests. The evaluator executed tests were sufficient to cover all of the security features claimed in the ST. The evaluation team also performed their own independently developed functional tests.

Finally, the evaluators performed tests for hypothesized vulnerabilities. The CCTL evaluation team determined that the vendor's own vulnerability analysis was thorough and appropriately tested. However, the evaluation team decided to supplement the vendor vulnerability analysis with some additional testing. The evaluation team performed a network scan on the test configuration using the NESSUS tool and performed some additional vulnerability tests based upon the results from the NESSUS report. The evaluator vulnerability testing determined that the postulated vulnerabilities were not present in the evaluated product.

The end result of the CCTL testing activities on the evaluated product was that all tests gave expected (correct) results. The final evaluator testing did not reveal any residual problems with the TOE. The testing found that the product was implemented as described in the functional specification. The CCTL evaluation team tests and penetration tests substantiated the security functional requirements claimed in the Security Target.

8 Evaluated Configuration

The evaluated version of the TOE was a configuration consisting of one Peakflow X Controller Version 3.1.4 and zero or more Peakflow X Collectors Version 3.1.4 deployed to collect and analyze network traffic. The evaluators actually tested in a configuration with precisely one Controller and one Collector.

8.1 Physical Boundaries

Both the Collector and Controller appliances are based on Intel commodity servers and utilize the Arbor Networks Operating System (ArbOS), which is based on OpenBSD. The entire appliances are within the TOE Physical Boundary. In addition, the TOE relies upon SSL to protect communication of TSF data between TOE components.

8.2 Logical Boundaries

The logical boundaries of the TOE can be described in terms of the security functions implemented in the TOE. Peakflow X implements security functions that support Identification & Authentication, Security Management, Protection of the TSF, and the Network Integrity System that are described in the Security Policy section of this report on page 4

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable International Interpretations in effect on 24 March 2004.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The final result was that the evaluation determined the product to be conformant with Part 2 extended and, as well, meeting the requirements for Part 3, and EAL 2. The details of the evaluation are recorded in the proprietary Evaluation Technical Report (ETR), [10] which is controlled by SAIC.

10 Validator Comments

All validator comments regarding this evaluated product are already captured in the Clarification of Scope section of this report on page 9.

There were no evaluator comments for the validator to pass on in this section of the report.

11 Security Target

The Security Target, "Arbor Peakflow X Security Target, Version 1.0, 8 July 2005" [9] is included here by reference.

12 List of Acronyms

ArbOS	Arbor Networks Operating System
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CM	Configuration Management
DSA	Directory System Agent
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICMP	Internet Control Message Protocol
IT	Information Technology
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OR	Observation Report
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Datagram Protocol

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

[9] Arbor Peakflow X Security Target, Version 1.0, dated 8 July 2005

[10] Evaluation Technical Report for Arbor Networks Peakflow X Version 3.1.4, (version 1.1) dated 2 November 2005